

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-134451

(43)Date of publication of application : 21.05.1999

(51)Int.Cl.

G06K 17/00
G06K 19/10

(21)Application number : 09-294441

(71)Applicant : NIPPON TELEGR & TELEPH CORP
<NTT>

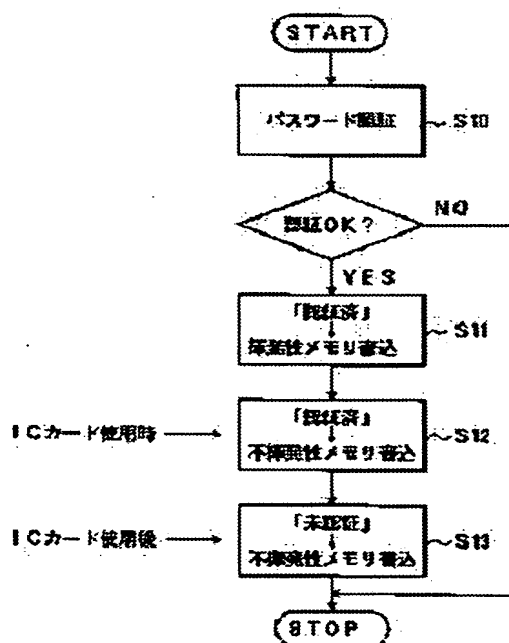
(22)Date of filing : 27.10.1997

(72)Inventor : MASUTSUKA KOUJI
YUSA HIROSHI
OMA YASUYUKI
SUZUKI KENICHI**(54) IC CARD, METHOD FOR CHANGING-OVER AUTHENTICATION OF IC CARD, SYSTEM THEREFOR AND RECORDING MEDIUM STORED WITH AUTHENTICATION CHANGE-OVER PROGRAM OF IC CARD**

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent a card from being used evilly by writing a usage possible state in a volatile memory at the time of inputting and authenticating a password, copying the contents of the volatile memory in a non-volatile memory after writing a usage impossible state at the time of pulling-out the card and holding the usage possible state at the time of pulling-out the card.

SOLUTION: The password is requested for the user of an IC card, authentication is executed based on the password which is inputted by the request (S10), 'authenticated' for adopting the IC card as the one in the usage possible state is written in the volatile memory at the time of authentication that a user is justified (S11) and 'authenticated' is also written in the non-volatile memory at the time of using the IC card (S12). Then, the contents of the volatile memory is copied into the non-volatile memory after using the IC card, 'not authenticated' is written in the non-volatile memory and the usage impossible state is held (S13). Thus, the card is prevented from being used evilly.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

4. Japanese Patent Application, Publication No.S62-177696
(No translation provided)

5. Japanese Patent Application, Publication No.H11-134451

[0031] Step 205) The terminal unit 30 performs a settlement process required for purchases or the like of a user, i.e., revises the balance corresponding to a relevant IC card (of a post payment account) by deducting the amount of these purchases or the like from it.

Step 206) When completing the settlement process, the terminal unit 30 executes the "CLEAR STATUS" command so as to have the content in the EEPROM 12 indicate the "yet-to-be-verified" state.

[0032] Step 207) When the user removes the IC card 10 from a card-slot of the terminal unit 30, the content in the RAM 11 changes automatically so as to indicate the "yet-to-be-verified" state as the power supply to the IC card stops. In this manner, it is possible for a user to use an IC card 10 at the terminal unit 30 located in a store without a need of going through a risk of entering his/her password in presence of other people even if the use of the IC card 10 is for a payment in a post payment system, and yet the card automatically turns into the "yet-to-be verified" state once the user completes the use this IC card. As result of this configuration, even if this IC card comes to a possession of other person, he/she cannot use the IC card as he/she does not know what a correct password is.

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平11-134451

(43)公開日 平成11年(1999)5月21日

(51)Int.Cl.⁸

識別記号

FI

G 0 6 K 17/00
19/10

G 0 6 K 17/00
19/00

T
R

審査請求 未請求 請求項の数11 OL (全 9 頁)

(21)出願番号 特願平9-294441

(22)出願日 平成9年(1997)10月27日

(71)出願人 000004226

日本電信電話株式会社

東京都新宿区西新宿三丁目19番2号

(72)発明者 益塚 幸児

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 遊佐 洋

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(72)発明者 大間 康之

東京都新宿区西新宿三丁目19番2号 日本
電信電話株式会社内

(74)代理人 弁理士 伊東 忠彦

最終頁に続く

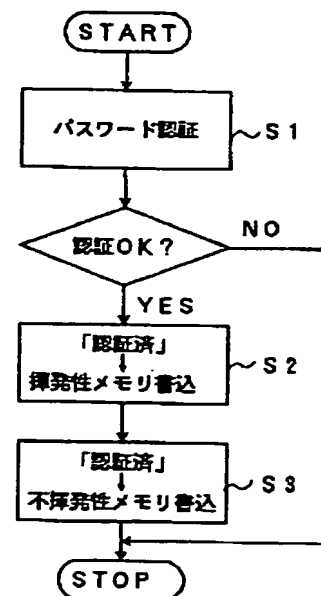
(54)【発明の名称】 ICカード及びICカードの認証切替方法及びシステム及びICカードの認証切替プログラムを格納した記憶媒体

(57)【要約】

【課題】 カードの所有者本人が本人確認を済ませた状態でICカードを保持しておく状態と、パスワード入力がないと使用不可能状態とする2通りの状態を選択することが可能なICカード及びICカードの認証切替方法及びシステム及びICカードの認証切替プログラムを格納した記憶媒体を提供する。

【解決手段】 本発明は、ICカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い、利用者が正当であると認証された場合に、前記ICカードを使用可能状態とする「認証済」を揮発性メモリに書き込む共に、前記不揮発性メモリにも「認証済」を書き込む。

本発明の第1の原理を説明するための図



【特許請求の範囲】

【請求項 1】 パスワードを入力し、認証することにより使用可能状態となる IC カードであって、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、前記揮発性メモリの内容が複写され、カード引抜き時においても使用可能状態を保持する不揮発性メモリとを有することを特徴とする IC カード。

【請求項 2】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替方法において、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い、前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込み、更に、前記不揮発性メモリにも「認証済」を書き込むことを特徴とする IC カード認証切替方法。

【請求項 3】 任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記 IC カードを使用不能状態とする「未認証」に書き替える請求項 2 記載の IC カード認証切替方法。

【請求項 4】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替方法において、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い、前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込み、前記 IC カードの使用時に、前記不揮発性メモリにも「認証済」を書き込み、前記 IC カードの使用後、前記不揮発性メモリに「未認証」を書き込むことを特徴とする IC カード認証切替方法。

【請求項 5】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替システムであって、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段と、前記認証手段により前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込み、更に前記不揮発性メモリ

にも「認証済」を書き込む認証情報書き込み手段とを有することを特徴とする IC カード認証切替システム。

【請求項 6】 任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記 IC カードを使用不能状態とする「未認証」に書き替える認証情報書き込み手段を更に有する請求項 5 記載の IC カード認証切替システム。

【請求項 7】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替システムであって、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段と、前記認証手段により、前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込む揮発性メモリ書き込み手段とを有するバランスリーダと、

前記 IC カードの使用時に、前記不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書き込み手段と、前記 IC カードの使用後、前記不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書き込み手段とを有する端末とを有することを特徴とする IC カード認証切替システム。

【請求項 8】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替プログラムを格納した記憶媒体であって、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、前記認証プロセスにより前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込み、更に前記不揮発性メモリにも「認証済」を書き込む認証情報書き込みプロセスとを有することを特徴とする IC カード認証切替プログラムを格納した記憶媒体。

【請求項 9】 任意のタイミングで、使用可能状態が書き込まれている前記不揮発性メモリの内容を、前記 IC カードを使用不能状態とする「未認証」に書き替える認証情報書き込みプロセスを更に有する請求項 8 記載の IC カード認証切替プログラムを格納した記憶媒体。

【請求項 10】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使

用不能状態とする IC カード認証切替プログラムを格納した記憶媒体であって、

前記 IC カードを読み込むバランスリーダに搭載され、前記 IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、

前記認証プロセスにより、前記利用者が正当であると認証された場合に、前記 IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込む揮発性メモリ書込プロセスとを有する IC カード認証切替プログラムを格納した記憶媒体。

【請求項 11】 パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替プログラムを格納した記憶媒体であって、

前記 IC カードの使用時の端末に搭載され、

前記 IC カードの使用時に、該 IC カードの前記揮発性メモリに「認証済」が書き込まれている場合に、前記不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込プロセスと、

前記 IC カードの使用後、前記不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込プロセスとを有することを特徴とする IC カード認証切替プログラムを格納した記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、IC カード及び IC カードの認証切替方法及びシステム及び IC カードの認証切替プログラムを格納した記憶媒体に係り、特に、IC カードの本人確認を行う場合における認証方法を切り替えるための IC カード及び IC カードの認証切替方法及びシステム及び IC カードの認証切替プログラムを格納した記憶媒体に関する。

【0002】

【従来の技術】図 10 は、従来の IC カードの構成を示す。従来、IC カード 10 を利用する場合には、当該 IC カード 10 を使用する毎に当該 IC カード 10 の所有者がパスワードを入力することで、本人性の確認を行っている。これにより IC カード 10 は、RAM 11 にパスワードが入力されて本人確認された後、使用可能状態となる。使用を終了する場合には、IC カード 10 をスロットから引き抜く（全て使用が終了すれば IC カードは返却口から出てくる）ことで、電源供給が絶たれ、本人確認情報の保持されている RAM は本人確認以前の状態（未認証状態）に戻る。

【0003】

【発明が解決しようとする課題】しかしながら、上記従来の方法に示すように、本人確認をカード使用の都度行

うことは、安全性の観点からは優れているが、利用する毎にパスワードを入力するため、利便性の観点からは本人確認をいちいち行うので面倒であるという問題がある。

【0004】本発明は、上記の点に鑑みなされたもので、カードの所有者本人が本人確認を済ませた状態で IC カードを保持しておく状態と、従来と同様に、パスワード入力がないと使用不可能状態とする 2 通りの状態を選択することが可能な IC カード及び IC カードの認証切替方法及びシステム及び IC カードの認証切替プログラムを格納した記憶媒体を提供することを目的とする。

【0005】

【課題を解決するための手段】本発明は、パスワードを入力し、認証することにより使用可能状態となる IC カードであって、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、揮発性メモリの内容が複写され、カード引抜き時においても使用可能状態を保持する不揮発性メモリとを有する。

【0006】図 1 は、本発明の第 1 の原理を説明するための図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替方法において、IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い（ステップ 1）、利用者が正当であると認証された場合に、IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込む共に（ステップ 2）、不揮発性メモリにも「認証済」を書き込む（ステップ 3）。

【0007】また、本発明は、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、IC カードを使用不可能状態とする「未認証」に書き替える。図 2 は、本発明の第 2 の原理を説明するための図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有する IC カードを、使用可能状態または、使用不能状態とする IC カード認証切替方法において、IC カードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行い（ステップ 10）、利用者が正当であると認証された場合に、IC カードを使用可能状態とする「認証済」を揮発性メモリに書き込み（ステップ 11）、IC カードの使用時に、不揮発性メモリにも「認証済」を書き込み（ステップ 12）、IC カードの使用後、不揮発性メモリに「未認証」を書き込む（ステップ 13）。

【0008】図 3 は、本発明の第 1 の原理構成図である。本発明は、パスワードが入力され、認証されると使

用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するICカードを、使用可能状態または、使用不能状態とするICカード認証切替システムであって、ICカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段21と、認証手段により利用者が正当であると認証された場合に、ICカードを使用可能状態とする「認証済」をICカードの揮発性メモリに書き込み、更に、不揮発性メモリにも「認証済」を書き込む認証情報書込手段22とを有する。

【0009】また、本発明のICカード認証切替システムは、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、ICカードを使用不能状態とする「未認証」に書き替える認証情報書替手段を更に有する。図4は、本発明の第2の原理構成図である。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するICカードを、使用可能状態または、使用不能状態とするICカード認証切替システムであって、ICカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証手段21と、認証手段により、利用者が正当であると認証された場合に、ICカードを使用可能状態とする「認証済」を揮発性メモリに書き込む揮発性メモリ書込手段23とを有するバランスリーダ20と、ICカードの使用時に、不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込手段33と、ICカードの使用後、不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込手段34とを有する端末30とを有する。

【0010】本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するICカードを、使用可能状態または、使用不能状態とするICカード認証切替プログラムを格納した記憶媒体であって、ICカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、認証プロセスにより利用者が正当であると認証された場合に、ICカードを使用可能状態とする「認証済」を揮発性メモリに書き込み、更に、不揮発性メモリにも「認証済」を書き込む認証情報書込プロセスとを有する。

【0011】また、本発明のICカード認証切替プログラムを格納した記憶媒体は、任意のタイミングで、使用可能状態が書き込まれている不揮発性メモリの内容を、ICカードを使用不能状態とする「未認証」に書き替える認証情報書替プロセスを更に有する。本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込

まれる揮発性メモリと、不揮発性メモリとを有するICカードを、使用可能状態または、使用不能状態とするICカード認証切替プログラムを格納した記憶媒体であって、ICカードを読み込むバランスリーダに搭載され、ICカードの利用者に対してパスワードを要求し、入力されたパスワードに基づいて認証を行う認証プロセスと、認証プロセスにより、利用者が正当であると認証された場合に、ICカードを使用可能状態とする「認証済」を揮発性メモリに書き込む揮発性メモリ書込プロセスとを有する。

【0012】本発明は、パスワードが入力され、認証されると使用可能状態が書き込まれ、カード引抜き時において使用不能状態が書き込まれる揮発性メモリと、不揮発性メモリとを有するICカードを、使用可能状態または、使用不能状態とするICカード認証切替プログラムを格納した記憶媒体であって、ICカードの使用時の端末に搭載され、ICカードの使用時に、該ICカードの揮発性メモリに「認証済」が書き込まれている場合に、不揮発性メモリにも「認証済」を書き込む使用時不揮発性メモリ書込プロセスと、ICカードの使用後、不揮発性メモリに「未認証」を書き込む使用後不揮発性メモリ書込プロセスとを有する。

【0013】上記のように、本発明は、不揮発性メモリと揮発性メモリを使い分けることにより、カードメモリの役割分担をすることで、カードの所有者が、本人確認を済ませた状態でカードを保持しておく場合と、従来のようにパスワード入力がないと使用可能状態にならない状態とを適宜選択できる構造を有する。即ち、ICカード内に揮発性メモリであるRAMと不揮発性メモリであるEEPROMの領域を設け、最初にパスワードにより本人確認してカード使用可能状態となったものを、EEPROMにそのまま保持し、次回からパスワードによる本人確認をしなくてもカードが使用できるようにした。EEPROMは、従来本人確認の状態を保持していたRAMと異なり、電源供給が絶たれても、メモリ内容は保持されるので、EEPROMに本人確認情報を保持させることで、カード所有者が、この本人確認情報を解除しない限り、本人確認することなくカード使用可能状態となる。但し、任意の時点でカード所有者の指示により、認証状態を解除することができる。

【0014】また、本発明では、上記において、任意に本人認証を解除できるが、解除しない場合は紛失した際に他人に使用される可能性がある。金額の限界を高く設定しているポストペイドのような場合には、何等かの形でガードをかける必要がある。つまり、EEPROMに保持されている本人認証情報を「未認証」にする必要がある。本発明では、EEPROMの認証済みの情報を自動的に未認証しているため、紛失してもパスワードの入力がない限り使われることはない。つまり、従来のカードは、パスワード入力を使用直前に端末を用いて入力し

なければならないが、本発明では、EEPROMにバランスリーダを用いて自分の家等のプライベートな場所を入力し、EEPROM上に認証済みの情報を保持しておき、店舗で買物等をしてカードを使用し、店舗の端末からカードを取り出す時にはRAM上にも“未認証”、EEPROM上でも“未認証”の状態となるようにすることで、パスワードを人前で入力することがない上に、使用後は、パスワードの入力なしには使用不能となるため、安全性を増すことができる。

【0015】

【発明の実施の形態】最初に本発明の第1の実施の形態について説明する。本実施形態では、最初にパスワードにより本人確認を行い、カード使用可能状態となったものを、EEPROMにそのまま“使用可能状態”として保持し、次回から本人確認を行わなくとも当該ICカードを利用できる形態であり、プリペイドカード等に適用される場合について説明する。

【0016】図5は、本発明のICカードの構成を示す。同図に示すRAM11には、当該ICカードの使用状態が書き込まれ、バランスリーダから引き抜かれた時点で当該RAM11の内容は消去される。EEPROM12は、ICカードの使用状態が書き込まれるとバランスリーダからICカードが引き抜かれた場合でも当該書き込まれた情報はそのまま保持される。

【0017】図6は、本発明の第1の実施形態におけるバランスリーダの構成を示す。同図に示すバランスリーダ20は、ICカードに対してパスワードを要求し、入力されたパスワードの認証を行う認証部21と、ICカードの状態を認証状態、未認証状態に切り替える切替制御部22から構成される。認証部21は、利用者にパスワードの入力要求を発行し、パスワードが入力されると当該ICカードの状態を未認証状態から認証状態にするために、ICカード10のRAM11を認証済とする。これにより、ICカード10では、RAM11に書き込まれた“認証済”をEEPROM12に対してコピーし、当該EEPROM12を認証状態として保持する。

【0018】切替制御部22は、上記の認証部21において“認証済”となっているEEPROMの状態を未認証にするためのステータスをICカード10に発行し、EEPROM22を“未認証”の状態とする。これにより、ICカード10をスロットから引き抜いた場合でも、ICカード10には“使用可能状態”が保持されるため、使用時にパスワードを入力する必要がない。

【0019】次に、本発明の第2の実施の形態を説明する。本実施形態は、ICカードの紛失や盗難に備えて、カード使用後に本人認証情報を“未認証”状態とする形態であり、ICカードが電子現金として利用されるような場合について説明する。図7は、本発明の第2の実施形態における店舗端末の構成を示す。

【0020】同図に示す店舗端末30は、ICカード1

0が“使用可能状態”（ICカード10内のEEPROM12の状態が“使用可能状態”）であり、電子現金として使用される場合に、購入した価格をICカード10の残高から差し引いて、その結果を新残高としてICカード10の内容を更新する支払制御部31と、ICカード10のEEPROM12の状態を“使用可能状態”から“使用不可能状態”に切り替えるステータスをICカード10に発行する切替制御部32から構成される。

【0021】

【実施例】以下、本発明の実施例を図面と共に説明する。

【第1の実施例】まず、第1の実施例として、ICカードとして使用限度額が予め決められているプリペイドカードを例として説明する。この場合、ICカードの所有者が本人確認を済ませた状態で当該カードを保持するものとする。

【0022】図8は、本発明の第1の実施例のプリペイドカードの使用例を示すシーケンスチャートである。

ステップ101) まず、バランスリーダ20がパスワードを取得すると、当該バランスリーダ20のスロットに挿入されたICカード（プリペイドカード）に記憶されているパスワードと入力されているパスワードとの照合を行い、照合において、一致する場合には、「VERIFY」コマンドを実行して、ICカード10のRAM11に認証情報として“認証済”を書き込む。

【0023】ステップ102) 次に、バランスリーダ20は、「STORE STATUS」コマンドを実行して、挿入されている当該ICカード10のEEPROM12に、RAM11の内容（“認証済”）をコピーする。

ステップ103) 当該ICカード10をバランスリーダ20のスロットから引抜くと、電源ストップによりRAM11の内容が自動的に“未認証”となる。

【0024】ステップ104) 当該ICカード10を所有者が使用する場合には、店舗端末30に当該ICカード10を挿入すると、端末30は、パスワードの入力要求を発行することなく、上位モジュールから「MOVE STATUS」を実行して当該ICカードのEEPROM12の内容をRAM11にコピーすることで、当該ICカード10が使用可能となる。

【0025】ステップ105) 端末30は、利用者の商品の購入等に対する金額を当該ICカード10に記憶されている額面から差し引く。

ステップ106) 決済が終了した利用者は、端末30からICカード10を引き抜くと、電源ストップにより自動的にRAM11の内容が“未認証”となる。

【0026】ステップ107) 利用者が自宅等のプライベートな場所に設置してあるバランスリーダ20に当該ICカード10を挿入すると、当該バランスリーダ20は、「CLEAR STATUS」コマンドを発行して当該ICカード10のEEPROM12の内容を“未認証”に書き

替える。このように、ICカード10のEEPROM12に「認証済」を書き込んでおくことにより、使用対象の端末においてパスワードの入力を行うことなく、当該端末において、当該カード10のEEPROM12の内容をRAM11にコピーすることにより使用可能となる。また、カード使用者の指示により任意の時点でバランスリーダ20により認証状態の解除（未認証状態）にすることが可能であるため、所有者が使用しない場合には、バランスリーダ20に当該ICカード10を挿入する処理を行うだけで、他人の悪意による使用が不可能となる。

【0027】【第2の実施例】次に、第2の実施例は、上記の第1の実施例におけるプリペイドカードの場合には、任意に本人認証を解除できるが、解除していない状態において紛失した際に、他人に使用される可能性が残る。特に金額の限界を高く設定しているポストペイドのような場合には、更なるガードが必要となる。

【0028】本実施例では、ICカードとしてポストペイド（電子現金）の場合を例として説明する。図9は、本発明の第2の実施例のポストペイドの使用例を示すシーケンスチャートである。

ステップ201） バランスリーダ20のスロットにICカード10を挿入すると、当該バランスリーダ20はパスワードの入力を要求し、パスワードが入力されると、当該ICカード10に記憶されているパスワードと入力されているパスワードとの照合を行う。

【0029】ステップ202） 照合において、一致する場合には「VERIFY」コマンドを実行してICカード10のRAM11に認証情報として「認証済」を書き込む。

ステップ202） 次に、「STORE STATUS」コマンドを実行して、バランスリーダ20は、挿入されている当該ICカード10のEEPROM12に、RAM11の内容（「認証済」）をコピーする。

【0030】ステップ203） 当該ICカード10をバランスリーダ20のスロットから引抜くと、電源ストップによりRAM11の内容が自動的に「未認証」となる。

ステップ204） 利用者が当該ICカード（ポストペイド）を使用する店舗端末30のスロットに挿入すると、当該端末30は、上位モジュールより「MOVESTATUS」コマンドを実行することにより、EEPROM12の内容（「認証済」）をRAM11にコピーする。これにより、当該ICカードが使用可能状態となる。

【0031】ステップ205） 端末30は、利用者の商品の購入等による決済を行い、当該ICカード（ポストペイド）の残金から決済金額を差し引いて、残金を更新する。

ステップ206） 決済が済むと、端末30は、「CLEAR STATUS」コマンドを実行して、EEPROM12の内

容を「未認証」とする。

【0032】ステップ207） 当該ICカード10を端末30のスロットから利用者が引き抜くと、電源ストップによりRAM11の内容が自動的に「未認証」となる。このように、店舗端末30においてポストペイドとしてICカード10を利用する場合にも、人前でパスワードの入力を行うことなく、当該カードが利用できると共に、利用が終了すると自動的に「未認証」状態となるので、仮に他者が拾って使用しようとしても、パスワードを入力しない限り使用することが不可能となる。

【0033】また、上記の第1及び第2の実施例では、プリペイドカード、ポストペイドを例としているが、この例に限定されることなく、認証、未認証のモードが必要となるICカード一般に適用可能である。また、図6、図7に示すバランスリーダや店舗端末の各構成要素をプログラムとして構築し、当該装置内のメモリや、フロッピーディスク、CD-ROM等の可搬記憶媒体に格納しておき、本発明のようにICカードの認証、未認証により使用を制限する必要があるシステムに汎用的に利用することが可能である。

【0034】なお、本発明は、上記の実施例に限定されることなく、特許請求の範囲内で種々変更・応用が可能である。

【0035】

【発明の効果】上述のように、本発明によれば、最初にパスワードにより本人確認を行いカード使用可能状態（「認証済」）となったものを、ICカード内の不揮発性メモリに保持しておくことで、カードリーダから引き抜くことにより電源の供給が絶たれ、揮発性メモリに格納されている本人確認情報が「未認証」であっても、使用時に改めてパスワードを入力することがないため、人前で本来秘密としておくべきパスワードの入力を行う必要がない。

【0036】さらに、使用後に、利用者の意思により再度不揮発性メモリに書き込まれている「認証済」の状態を「未認証」に書き替えることも可能であり、利用者の意思により適宜いずれかの状態を選択することが可能である。また、本発明によれば、プライベートな場所でパスワードを入力し、不揮発性メモリに「認証済」を保持しておき、当該カードの使用後、当該不揮発性メモリの状態を「未認証」と書き替えることにより、店舗端末からカードを取り出す時点では、揮発性メモリ及び不揮発性メモリの双方が「未認証」状態となるため、と該カードの悪用が回避できる。

【図面の簡単な説明】

【図1】本発明の第1の原理を説明するための図である。

【図2】本発明の第2の原理を説明するための図である。

【図3】本発明の第1の原理構成図である。

【図4】本発明の第2の原理構成図である。

【図5】本発明のICカードの構成図である。

【図6】本発明の第1の実施形態におけるバランスリーダの構成図である。

【図7】本発明の第2の実施形態における店舗端末の構成図である。

【図8】本発明の第1の実施例のプリペイドカードの使用例を示すシーケンスチャートである。

【図9】本発明の第2の実施例のポストペイドの使用例を示すシーケンスチャートである。

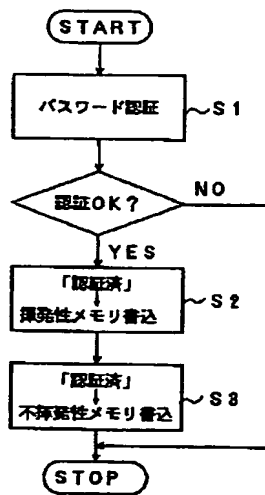
【図10】従来のICカードの構成図である。

【符号の説明】

- 10 ICカード
- 11 RAM
- 12 EEPROM
- 20 バランスリーダ、ICカード認証切替システム
- 21 認証部、認証手段
- 22 切替制御部、認証情報書込手段
- 23 揮発性メモリ書込手段
- 30 店舗端末
- 31 支払制御部
- 32 切替制御部
- 33 使用時不揮発性メモリ書込手段
- 34 使用后不揮発性メモリ書込手段

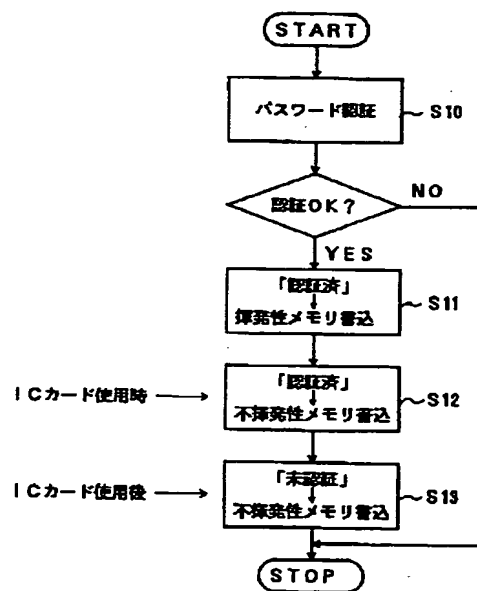
【図1】

本発明の第1の原理を説明するための図



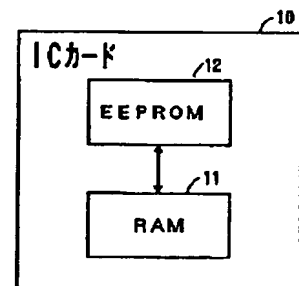
【図2】

本発明の第2の原理を説明するための図



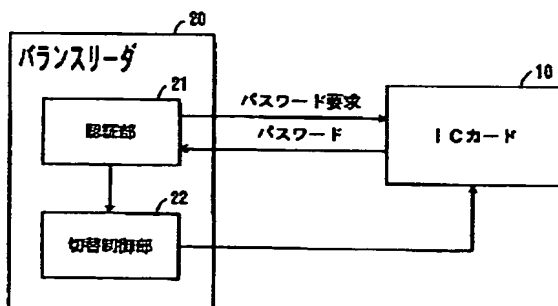
【図5】

本発明のICカードの構成図



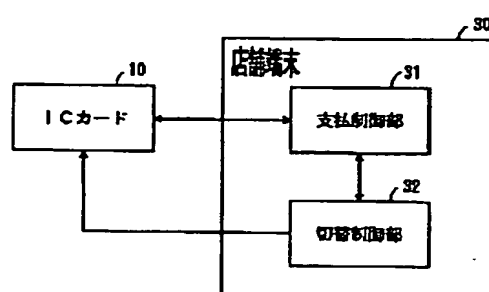
【図6】

本発明の第1の実施形態におけるバランスリーダの構成図



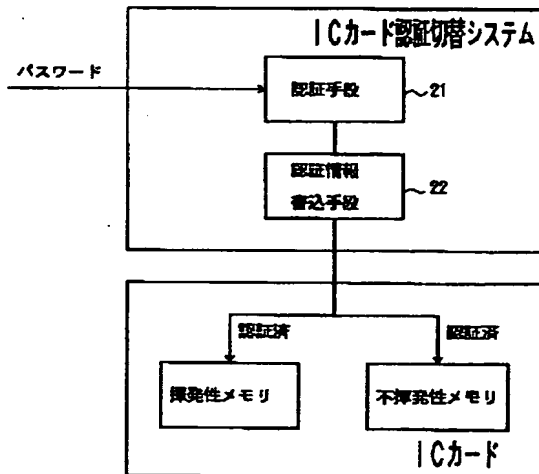
【図7】

本発明の第2の実施形態における店舗端末の構成図



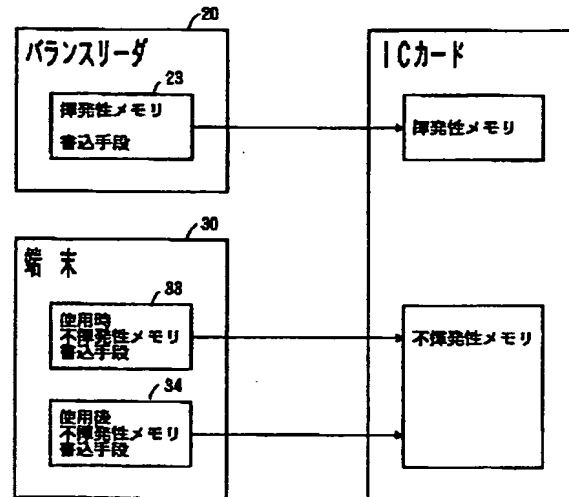
【図 3】

本発明の第 1 の原理構成図

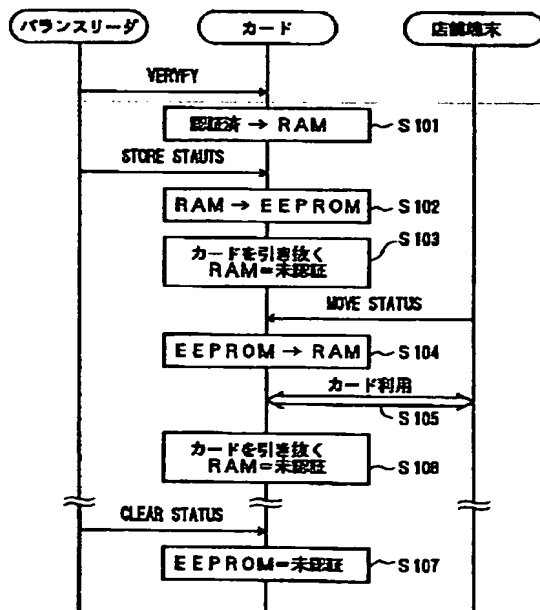


【図 4】

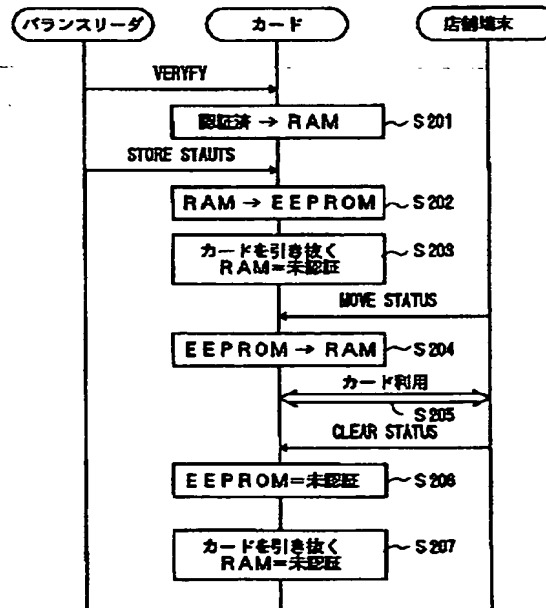
本発明の第 2 の原理構成図



【図 8】

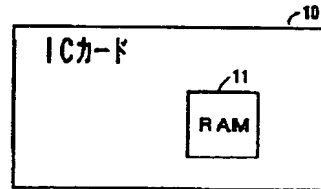
本発明の第 1 の実施例のプリペイドカードの
使用例を示すシーケンスチャート

【図 9】

本発明の第 2 の実施例のポストペイドの
使用例を示すシーケンスチャート

【図 10】

従来の IC カードの構成図



フロントページの続き

(72) 発明者 鈴木 健一

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内